

1
2
3
4
5
6
7
8 **UNITED STATES DISTRICT COURT**
9 **SOUTHERN DISTRICT OF CALIFORNIA**

10 UNITED STATES OF AMERICA,

11 Plaintiff,

12 vs.

13 BASAALY MOALIN; MOHAMED
14 MOHAMED MOHAMUD; ISSA
DOREH; AHMED NASIR TAALIL
MOHAMUD,

15 Defendants.

CASE NO. 10cr4246 JM

AMENDED ORDER DENYING
MOTION FOR NEW TRIAL

16
17 The court issues this Amended Order Denying Motion for New Trial to correct
18 a factual misstatement in its November 14, 2013 Order Denying Motion for New Trial
19 (“Order”). (Ct. Dkt. 386). The court deletes the phrase “and the telephony metadata
20 collected from the NSA program was either provided,” (Ct. Dkt. 386 at p.7:15-16), and
21 replaces it with “and the telephony metadata, collected pursuant to the FISA warrants
22 and subpoenaed telephone toll records, was either provided.” The Amended Order
23 follows:

24 Defendants Basaaly Moalin (“Moalin”), Mohamed Mohamed Mohamud
25 (“Mohamud”), Issa Doreh (“Doreh”), and Ahmed Nasir Taalil Mohamud (“Nasir”)
26 jointly move for a new trial pursuant to Federal Rule of Criminal Procedure 33. The
27 Government opposes the motion. Having carefully considered the papers submitted,
28 the court record, and the arguments of counsel, the court denies the motion for new

1 trial.

2 **BACKGROUND**

3 **The Second Superseding Indictment**

4 Filed on June 8, 2012, the operative Second Superseding Indictment alleges five
5 counts: (1) conspiracy to provide material support to terrorists in violation of 18 U.S.C.
6 §2339A(a); (2) conspiracy to provide material support to a foreign terrorist
7 organization in violation of 18 U.S.C. §2339B(a)(1); (3) conspiracy to launder
8 monetary instruments in violation of 18 U.S.C. §1956(h); (4) providing material
9 support to terrorists in violation of 18 U.S.C. §2339A(a); and (5) providing material
10 support to a foreign terrorist organization in violation of 18 U.S.C. §§2339B(a)(1) and
11 (2). (Ct. Dkt. 147). Counts One, Two and Three were charged against all Defendants,
12 Count Four against Moalin alone, and Count Five against all Defendants except Nasir.

13 **The FISA Motion**

14 On December 9, 2011, Defendants, among other things, moved to suppress
15 wiretap evidence obtained pursuant to a Foreign Intelligence Surveillance Act
16 (“FISA”) warrant, evidence seized pursuant to a search warrant of Defendant Moalin’s
17 home; and statements made at the time of Defendant Moalin’s arrest. (Ct. Dkt. 92).
18 On October 17, 2012, the court issued an order denying the motion to suppress
19 evidence seized from Moalin’s residence, denied the motion to suppress statements,
20 and continued the FISA wiretap motion.

21 Defendants’ FISA motion challenged the Government’s use of electronic
22 surveillance obtained pursuant to 50 U.S.C. §1806 (Title I of FISA) and those
23 collections obtained after the enactment of Section 702 (50 U.S.C. §1881a) of the FISA
24 Amendments Act of 2008 (“FAA”). On June 4, 2012, in an order placed under seal
25 with the Court Security Officer (“FISA Order”), the court denied Defendants’ motion
26 to suppress FISA intercepts and provided the parties notice of that fact. (Ct. Dkt. 146).

27 On March 9, 2012, in reply to the Government’s opposition to the motion to
28 dismiss FISA materials, Defendants repeated their request that defense counsel

1 possessing appropriate security clearances be granted access to the FISA warrant
2 applications and pertinent orders of the Foreign Intelligence Surveillance Court
3 (“FISC”). Among other things, Defendants argued that the electronic surveillance was
4 obtained in violation of FISA, the First and Fourth Amendments, and Brady v.
5 Maryland, 373 U.S. 83 (963). Defendants also argued that the minimization protocols
6 were defective. (Ct. Dkt. 131).

7 8 **The CIPA Motions**

9 On March 9, 2012, Defendants jointly and preemptively moved to deny the
10 Government’s anticipated request for an ex parte and in camera review pursuant to
11 Section 4 of the Classified Information Protection Act (“CIPA”), 18 U.S.C. App. 3 §4.
12 On March 23, 2012, the Government filed a response to Defendants joint motion to (1)
13 deny the ex parte CIPA filing and (2) compel disclosure of the CIPA materials to
14 cleared defense counsel. To assist the court in its review of CIPA-related materials for
15 purposes of Brady, the First and Fourth Amendments, Fed.R.Crim.P. 16, and the Jencks
16 Act, the court requested, and Defendants jointly submitted under seal, a memorandum
17 identifying seven broad defense theories as well as specific evidence sought to be
18 discovered in the Government’s CIPA submission. (Ct. Dkt 133-35).

19 Ultimately, the Government submitted five requests for a protective order under
20 CIPA. On August 28, 2012, the court completed its CIPA review of the materials
21 provided by the Government and dated March 21, 2012, June 1, 2012, and August 22,
22 2012.¹ On August 28, 2012, the court filed its first CIPA order under seal with the
23 Court Security Officer and provided notice to all parties of its entry. The court also
24 ordered the Government to provide to Defendants two substituted statements as
25 permitted by CIPA. (Ct. Dkt. 183). On January 17, 2013, the court granted the motion
26 for a protective order concerning two additional submissions by the Government and

27
28 ¹ Upon completion of its initial review of the submitted CIPA materials, the court
requested in a sealed order that the Government submit additional classified documents
for in camera review.

1 dated January 2, 2013, and January 17, 2013. (Ct. Dkt. 253).

2 On January 28, 2013, Defendants filed under seal a motion for Court Ordered
3 Remedies to Address the Government's Violation of Brady. (Ct. Dkt 271). On January
4 30, 2013, the court issued an order addressing several discovery-related issues raised
5 in Defendants' motion and requesting that the Government submit for in camera review
6 the redacted emails at issue. (Ct. Dkt. 273). Ultimately, the court concluded that the
7 unredacted emails need not be produced pursuant to Brady, Fed.R.Crim.P. 16, or the
8 Jencks Act. (Ct. Dkt. 279).

9 **The Rule 15 Depositions**

10 On July 20, 2012, Defendants filed a second motion to take the depositions of
11 eight prospective defense witnesses in Somalia. (Ct. Dkt. 154). Defendants
12 represented that these individuals received money transfers from Defendant Moalin and
13 possessed direct knowledge of how the transferred money was spent. (Ct. Dkt. 154 at
14 p.2:13-14). The court denied the motion without prejudice and referred the parties to
15 Magistrate Judge William V. Gallo to discuss the Rule 15 depositions. On September
16 6, 2012, after consulting with the parties, Magistrate Judge Gallo ordered the eight
17 depositions to proceed in Djibouti, Djibouti, (Ct. Dkt. 189), and set forth the logistics
18 for the witness depositions. (Ct. Dkt. 195). The depositions (except the deposition of
19 Farah Shidane) went forward in Djibouti from November 11-15, 2012. The videotaped
20 depositions were viewed by the jury during Defendants' case-in-chief.

21 **The Trial**

22 The jury trial commenced on January 28, 2013. The Government presented 13
23 witnesses over five days and the Defense presented 11 witnesses over five days,
24 including eight video-taped depositions taken pursuant to Fed.R.Crim.P. 15(a). On
25 February 22, 2013, after 17 days of trial and deliberations, the jury returned guilty
26
27
28

1 verdicts on all counts alleged in the second superseding indictment.²

2 **Recent Public Disclosures**

3 On June 8, 2013, The Washington Post reported on disclosures made by Edward
4 Snowden, a former NSA contract employee. As described by Defendants, “[t]he
5 documents Mr. Snowden provided revealed the existence of the scope of NSA’s
6 electronic surveillance, interception, and collection, including communications data
7 relevant to U.S. persons.” (Motion at p.7:12-14). In broad brush, the disclosures
8 revealed the existence of several classified United States surveillance programs and
9 their scope. As reported by the Associated Press, on September 26, 2013, NSA director
10 Keith B. Alexander confirmed that one goal of the NSA is to collect and store all phone
11 records of American citizens. Senators: Limit NSA Snooping into US Phone Records,
12 Associated Press, October 15, 2013.

13 In addition to the so-called Snowden disclosures, Defendants also cite several
14 statements made by Sean Joyce, Deputy Director of the FBI, before the House
15 Permanent Select Committee on Intelligence to support their Rule 33 motion.
16 Defendants highlight that Deputy Director Joyce stated that material obtained from the
17 NSA program resulted in the investigation of terrorist activities, including the present
18 case. (Def’t Exh. 2). Deputy Director Joyce also stated that the NSA provided a
19 telephone number in San Diego “that had indirect contact with an extremist outside the
20 United States.” Using this telephone number the FBI “served legal process to identify
21 the subscriber to this telephone number.” He further stated, “However, the NSA using
22 the business record FISA [Section 215] tipped us off that this individual had indirect
23 contacts with a known terrorist overseas.” Based largely upon this investigation, the
24 FBI applied to the FISC for FISA warrants and “disrupt[ed] this terrorist activity.” Id.

25 On July 18, 2013, at a conference at the Aspen Security Forum in Aspen
26 Colorado, General Alexander reportedly repeated that, based on information obtained

27
28 ² On September 21, 2012, the court appointed Magistrate Judge Gallo as a
special master to oversee the depositions and authorized the Magistrate Judge to
exercise those duties specifically enumerated in Fed.R.Civ.P. 53(c).

1 in Somalia, a telephone number was traced to San Diego. The telephone number was
2 traced to Defendant Moalin and an investigation was commenced against him “in 2003
3 but didn’t have enough information to go up on.” (Def’t Exh. 3).

4 On July 31, 2013, Deputy Director Joyce provided testimony before the Senate
5 Judiciary Committee. He reportedly stated that an FBI investigation of Defendant
6 Moalin was opened “in 2003 based on a tip. We investigated that tip. We found no
7 nexus to terrorism and closed the case.” (Def’t Exh. 5). He also stated that, in 2007,
8 the NSA advised the FBI that the San Diego telephone number was in contact with
9 members of al-Shabaab.³ Acting on this information, the FBI “served legal process to
10 identify the unidentified phone number. We identified [Defendant Moalin].” Id.

11 **Classified Facts Summary**

12 The court incorporates the classified factual summary set forth in the
13 Government’s opposition filed under seal.

14 **DISCUSSION**

15 **Legal Standards**

16 The court notes that neither Defendants nor the Government sets forth the legal
17 standard governing this motion. Under Rule 33(a), the court has broad authority to
18 grant a motion for new trial whenever “the interest of justice so requires.”
19 Fed.R.Crim.P. 33(a); United States v. Young, 17 F.3d 1201, 1205 (9th Cir. 1994).
20 Notably, Defendants raise no typical arguments for a new trial: sufficiency of the
21 evidence, evidentiary rulings, instructional challenge, or prosecutorial misconduct.
22 Rather, Defendants focus on two sealed orders of the court: the order denying the
23 motion to suppress FISA intercepts and the order granting the Government’s motion
24 for a protective order under CIPA.

25 ³ Al-Shabaab, a violent and brutal militia group, was designated by the U.S.
26 Department of State as a Foreign Terrorist Organization on February 26, 2008. (Ct.
27 Dkt. 147 ¶1). “Throughout al-Shabaab’s war against the TFG (Somalia’s Transitional
28 Federal Government) and its Ethiopian and African Union supporters, al-Shabaab used
harassment and targeted assassinations of civilians, improvised explosive devices,
mines, mortars, automatic weapons, suicide bombings, and general tactics of
intimidation and violence.” Id. ¶2).

1 Defendants broadly argue that recent revelations by Snowden and Government
2 officials regarding NSA surveillance in this particular case warrant the suppression of
3 all intercepted conversations. Although the present motion does not neatly fit into the
4 category of newly discovered evidence, it is nonetheless helpful to set forth the
5 standard for such a claim. The court considers the following five part test to determine
6 whether to grant a new trial based on newly discovered evidence: (1) the evidence must
7 be newly discovered; (2) the failure to discover the evidence sooner must not be the
8 result of a lack of diligence on the defendant's part; (3) the evidence must be material
9 to the issues at trial; (4) the evidence must be neither cumulative nor merely
10 impeaching; and (5) the evidence must indicate that a new trial would probably result
11 in acquittal. Untied States v. Sarno, 73 F.3d 1470, 1507 (9th Cir. 1995).

12 Setting aside the issue of admissibility of the public revelations of the NSA
13 program of securing telephone metadata, the public disclosure of the NSA program
14 adds no new facts to alter the court's FISA and CIPA rulings. Because the court has
15 already considered and addressed many of the FISA and CIPA arguments from a
16 federal and constitutional law perspective, the present motion is akin to a motion for
17 reconsideration. Under the reconsideration standard, the court is authorized to alter its
18 prior rulings based upon newly discovered evidence, intervening change of law, or
19 clear error. See School Dist. N. 1J, Multnomah Cty. v. ACandS, Inc., 5 F.3d 1255,
20 1262 (9th Cir. 1993). The court notes that the newly discovered evidence prong is not
21 particularly useful in this case to the extent the NSA revelations are newly discovered
22 by Defendants. The mere existence of the NSA program has no evidentiary value in
23 and of itself, and the telephony metadata, collected pursuant to the FISA warrants and
24 subpoenaed telephone toll records, was either provided to the defense by means of the
25 intercepted telephone calls produced in discovery or considered by this court under its
26 FISA and CIPA responsibilities. Similarly, the intervening change of law prong is not
27 useful to the Defendants because they cite no intervening change of law. To the extent
28 the clear error prong applies, the court notes that the clear error standard is analogous

1 to the “interests of justice” requirement of Rule 33.

2 **The Motion**

3 Defendants raise three main arguments in support of their motion for new trial:
4 (1) The NSA intercepts and/or collection of electronic data related to Defendant Moalin
5 violated the First and Fourth Amendments and FISA; (2) cleared defense counsel
6 should have previously been, and, should now be provided with the Government’s
7 under seal response to their FISA motion, including the FISA applications and
8 warrants, and the ex parte request for a protective order under CIPA; and (3) the
9 Government failed to provide necessary Rule 16 discovery and exculpatory materials
10 under Brady. To the extent possible, each argument is discussed in this publicly
11 available order.⁴

12 The NSA Surveillance

13 Defendants argue that the collection of telephony metadata violated Defendant
14 Moalin’s First and Fourth Amendment rights. At issue are two distinct uses of
15 telephone metadata obtained from Section 215. The first use involves telephony
16 metadata retrieved from communications between third parties, that is, telephone calls
17 not involving Defendants. Clearly, Defendants have no reasonable expectation of
18 privacy to challenge any use of telephony metadata for calls between third parties. See
19 Steagald v. United States, 451 U.S. 204, 219 (1981) (Fourth Amendment rights are
20 personal in nature); Rakas v. Illinois, 439 U.S. 128, 133-34 (1978) (“Fourth
21 Amendment rights are personal rights which, like some other constitutional rights, may
22 not be vicariously asserted.”); United States v. Verdugo-Urquidez, 494 U.S. 259, 265
23 (1990) (the term “people” described in the Fourth Amendment are persons who are part
24 of the national community or may be considered as such). As noted in Steagald, “the
25 rights [] conferred by the Fourth Amendment are personal in nature, and cannot bestow
26 vicarious protection on those who do not have a reasonable expectation of privacy in

27
28 ⁴ The court informs the parties that this is the only order addressing the issues
raised in the Rule 33 motion. No order has been filed under seal to address
Defendants’ arguments.

1 the place to be searched.” 451 U.S. at 219. As individuals other than Defendants were
2 parties to the telephony metadata, Defendants cannot vicariously assert Fourth
3 Amendment rights on behalf of these individuals. To this extent, the court denies the
4 motion for new trial.

5 The second use of telephony metadata involves communications between
6 individuals in Somalia (or other countries) and Defendant Moalin. The following
7 discusses whether Defendant Moalin, and other Defendants through him, have any
8 reasonable expectation of privacy in telephony metadata between Moalin and third
9 parties, including co-defendants.

10 **The Fourth Amendment**

11 Defendants contend that they have a Fourth Amendment reasonable expectation
12 of privacy in the collection of telephony metadata for communications between third
13 parties and Defendants.⁵ In Smith v. Maryland, 442 U.S. 735 (1979), the Supreme
14 Court addressed whether the Fourth Amendment was violated when the telephone
15 company, at police request and without a warrant, installed a pen register to record
16 numbers dialed from petitioner Smith’s home. Based upon information received from
17 the victim, the police believed that Smith was involved in a robbery. After the robbery,
18 the victim received threatening and obscene telephone calls from an individual
19 identifying himself as the robber. Id. at 737. The device installed recorded the
20 telephone numbers dialed from the defendant’s home but did not record the contents
21 of the conversation. When the victim received another telephone call from Smith, the
22 police obtained a search warrant to search Smith’s home.

23 Consistent with Katz v. United States, 389 U.S. 347 (1967), the Supreme Court
24 held that the application of the Fourth Amendment “depends on whether the person
25 invoking its protection can claim a ‘justifiable,’ a ‘reasonable,’ or a ‘legitimate
26 expectation of privacy’ that has been invaded by government action.” Smith, 442 U.S.

27
28 ⁵ The Fourth Amendment guarantees “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”

1 at 740. A justifiable, reasonable, or legitimate expectation of privacy is one where (1)
2 the defendant, by his conduct, has “exhibited an actual (subjective) expectation of
3 privacy,” and (2) the individual’s subjective expectation of privacy is “one that society
4 is prepared to recognize as ‘reasonable,’” that is, whether the individual’s expectation,
5 “viewed objectively is ‘justifiable under the circumstances.’” Id. (quoting Katz, 389
6 U.S. at 351-62).

7 The Supreme Court noted that someone who uses a telephone has “‘voluntarily
8 conveyed numerical information to the telephone company and exposed’ that
9 information to its equipment in the ordinary course of business,” and therefore has
10 “assumed the risk that the company would reveal to police the numbers he dialed.” Id.
11 at 744. The Supreme Court has consistently held “that a person has no legitimate
12 expectation of privacy in information he voluntarily turns over to third parties.” Id.;
13 United States v. Miller, 425 U.S. 435 (1976) (“the Fourth Amendment does not prohibit
14 the obtaining of information revealed to a third party and conveyed by him to United
15 States authorities, even if the information is revealed on the assumption that it will be
16 used only for a limited purpose and the confidence placed in the third party will not be
17 betrayed”).

18 In United States v. Reed, 575 F.3d 900 (9th Cir. 2009), the Government, acting
19 without a warrant, requested that the telephone company install a pen register and trap
20 and trace device on the defendant’s telephone. The pen register and trap and trace
21 device provided “call data content,” that is, data about “call origination, length, and
22 time.” Id. at 914. The defendants argued that the call data content had to be
23 suppressed under the Fourth Amendment. Citing Smith, the Ninth Circuit determined
24 that defendants had no Fourth Amendment “expectation of privacy” in the data and
25 affirmed the district court’s denial of the motion to suppress. Id. Further, the Ninth
26 Circuit has repeatedly held that an individual does not have a reasonable expectation
27 of privacy in business records such as power company consumption records, telephone
28 records, bank records, or motel registration records. United States v. Golden Valley

1 Elec. Ass’n, 689 F.3d 1108, 1116 (9th Cir. 2012); United States v. Miller, 425 U.S.
2 436, 440 (1976) (“the Fourth Amendment does not prohibit the obtaining of
3 information revealed to a third party and conveyed by him to the United States
4 authorities”); United States v. Phibbs, 999 F.2d 1053, 1077 (6th Cir. 1993) (holding it
5 was “evident” that the defendant did not have any justifiable privacy interest in
6 telephone records obtained from the service provider); United States v. Qing Li, 2008
7 WL 789899 *4 (S.D. Cal. Mar. 20, 2008, No. 07cr2915 JM) (defendant lacks a
8 reasonable expectation of privacy in Internet Protocol log-in histories and addressing
9 information).

10 In light of these persuasive and binding authorities, Defendants argue that the
11 court should blaze a new path and adopt the approach to the concept of privacy set
12 forth by Justice Sotomayor in her concurrence in United States v. Jones, ___ U.S. ___, 132
13 S.Ct. 945, 954-964 (2012). In Jones, the Supreme Court considered whether the
14 installation and subsequent monitoring of a Global Positioning System tracking device
15 on an automobile by the police without a valid warrant and without the individual’s
16 consent violated the Fourth Amendment. Noting that Fourth Amendment
17 jurisprudence, up to the latter half of the 20th century, was tied to common-law trespass
18 principles, the majority held that “[w]here, as here, the Government obtains information
19 by physically intruding on a constitutionally protected area,” the Fourth Amendment
20 is violated. Id. at 950 n.3, 954. As noted by Defendants, Justice Sotomayor stated that
21 the recent rise of the digital era of cell phones, internet, and email communications may
22 ultimately require a reevaluation of “expectation of privacy in information voluntarily
23 disclosed to third parties.” Id. at 957. Defendants extrapolate from this dicta that the
24 court should recognize that Defendant Moalin had a reasonable expectation of privacy
25 cognizable under the Fourth Amendment that the Government would not collect either
26 individual or aggregated metadata.

27 The difficulty with Defendants’ argument is twofold. First, the use of pen
28 register-like devices - going back to Samuel Morses’s 1840 telegraph patent - predates

1 the digital era and cannot be considered a product of the digital revolution like the
2 internet or cell phones. See Samuel F.G. Morse, Improvement in the Mode of
3 Communicating Information by Signals by the Application of Electro-Magnetism, U.S.
4 Patent 1647, June 20, 1840, page 4 column 2. In short, pen register-like devices
5 predate the internet era by about 150 years and are not a product of the so-called digital
6 revolution - the basis for the concerns articulated by Justice Sotomayor. Second, and
7 more importantly, the Supreme Court specifically and unequivocally held in Smith that
8 retrieval of data from a pen register by the Government without a search warrant is not
9 a search for Fourth Amendment purposes. 442 U.S. at 744. Because individuals
10 voluntarily convey numerical information to the telephone company to complete a
11 telephone call, one cannot possess a reasonable expectation of privacy in the telephone
12 number dialed (as opposed to the content of the conversation). Id. For these reasons,
13 the court declines Defendants' invitation to depart from well-established precedent.

14 Here, when Defendant Moalin used his telephone to communicate with third
15 parties, whether in Somalia or the United States, he had no legitimate expectation of
16 privacy in the telephone numbers dialed. The calls were routed through the
17 communications company and its switching equipment in the ordinary course of
18 business. While Defendant Moalin may have had some degree of a subjective
19 expectation of privacy, that expectation is not "one that society is prepared to recognize
20 as reasonable." Rakas v. Illinois, 439 U.S. 128, 143-44 n.12 (quoting Katz, 389 U.S.
21 at 361). Furthermore, where the calls were initiated by third parties, whether from
22 Somalia or other countries, Defendant Moalin's subjective expectation of privacy is
23 even further diminished because Defendant Moalin cannot assert Fourth Amendment
24 principles on behalf of third parties. The court could not locate any authorities, nor do
25 Defendants cite any pertinent authorities, that recognize any expectation of privacy in
26 the receipt of telephone call data from a third party in a foreign country. As in Smith,
27 because the metadata was obtained through communications companies and their
28 switching equipment, Defendant Moalin "cannot claim that his property was invaded

1 or that police intruded into a ‘constitutionally protected area.’” 442 U.S. at 741.⁶
2 While technology continues to advance through the implementation of new devices and
3 methods, the legal analysis remains fairly constant: whether “the government violate[d]
4 a subjective expectation of privacy that society recognizes as reasonable.” Kyllo v.
5 United States, 533 U.S. 27, 33 (2001). For the above stated reasons, Defendant’s
6 minimal subjective belief in the privacy of telephony metadata is not one that society
7 has adopted.

8 The FISC has similarly determined that individuals like Defendant Moalin
9 cannot successfully assert a cognizable Fourth Amendment claim to telephony
10 metadata. In In re Application of the Federal Bureau of Investigation for an Order
11 Requiring the Production of Tangible Things, 2013 WL 5307991, *3 (For. Intell. Sur.
12 Ct. Aug. 29, 2013), the court found that a Section 215 order for telephony metadata
13 does not implicate the Fourth Amendment.

14 [B]ecause the Application at issue here concerns only the production of
15 call detail records or ‘telephony metadata’ belong to a telephone company,
16 and not the contents of communications, Smith v. Maryland compels the
17 conclusion that there is no Fourth Amendment impediment to the
collection [T]his court finds that the volume of records being
acquired does not alter this conclusion. Indeed, there is no legal basis for
the Court to find otherwise.

18 Defendants also vigorously contend that “the long-term recording and
19 aggregation of telephony metadata constitutes” an impermissible Fourth Amendment
20 search. (Reply at p. 6:7-8). The court notes that the preservation of “long-term
21 recordings” of telephony metadata played a minor role in the underlying
22 investigations.⁷ At the time of oral argument, defense counsel argued that Jewel v.

24 ⁶ As set forth above, Defendant Moalin lacks standing to challenge the metadata
25 collected in reference to communications initiated by third parties. The Fourth
26 Amendment rights are “personal in nature” and Defendant Moalin cannot assert any
Fourth Amendment right on behalf of any party subject to the collection of telephone
metadata. See Steagald, 451 U.S. 204, 219.

27 ⁷ The court declines to reach Defendants’ generalized arguments that (1) the
28 NSA involvement in surveillance activities was overbroad or (2) the NSA violated
orders by the FISC. Such public revelations and the ensuing debates in public and
political arenas do not alter or lessen this court’s responsibility to apply constitutional

1 National Sec. Agency, 673 F.3d 902 (9th Cir. 2011) supports their position. There, the
2 plaintiff filed a putative class action on behalf of all Americans who were subscribers
3 of AT&T. Plaintiff alleged that the Government attached surveillance devices to
4 AT&T's network. Id. at 906. The district court dismissed the action on standing
5 grounds. The central, merits-based allegation in Jewel arose "from claims that the
6 federal government, with the assistance of major telecommunications companies,
7 engaged in widespread warrantless eavesdropping in the United States following the
8 September 11, 2001, attacks." Id. at 905. Shortly after the 911 attacks, President Bush
9 authorized "a terrorist surveillance program to detect and intercept al Qaeda
10 communications involving someone here in the United States." Id. at 912. Plaintiff
11 alleged that the Government acquired the content of all email, internet, and telephone
12 communications. The court concludes that Jewel is not helpful to Defendants. First,
13 the merits involved the alleged eavesdropping on the content of the communications,
14 not just the telephony metadata. Second, the issues addressed in Jewel related to
15 standing, and not the Fourth Amendment. Id. at 905 (the issue is whether the plaintiff
16 had "standing to bring their statutory and constitutional claims").

17 In sum, the court denies the motion for new trial based upon the alleged violation
18 of the Fourth Amendment.

19 **The First Amendment**

20 Defendants raise a generalized First Amendment challenge. In broad brush,
21 Defendants argue that "the 2003 investigation of Mr. Moalin 'did not find any
22 connection to terrorist activity.' It is inconceivable that the investigation did not also
23 involve investigation of conduct and/or expression by Mr. Moalin fully protected by
24 the First Amendment." (Reply at p.15:12-14). Defendants cite no evidence nor
25 provide legal authority to support the proposition that Defendant Moalin's First
26 Amendment rights were violated in any manner.

27 In sum, the court denies the motion for new trial based upon the alleged violation
28 _____
and other relevant legal principles to this motion.

1 of the First Amendment.

2 The FISA and CIPA Section 4 Arguments

3 Defendants argue that the Government did not comply with the provisions of
4 FISA and CIPA. The FISA and CIPA challenges are not addressed herein but in the
5 court's previous sealed orders. With respect to the FISA and CIPA challenges, the
6 court notes that the arguments do not identify any newly discovered evidence,
7 intervening change in law, or clear error warranting reconsideration of its FISA and
8 CIPA orders.

9 In sum, the court denies the motion for new trial based upon the alleged violation
10 of FISA and CIPA.

11 Renewed Motion to Gain Access to FISA and CIPA Materials

12 In a well-presented argument, Defendants contend that cleared defense counsel
13 should have been earlier and should now be provided with all CIPA and FISA-related
14 materials (including FISA applications, exhibits, and FISC orders). Legal authorities
15 that have addressed this precise issue have uniformly rejected this argument. While
16 counsel may have security clearances, classified information may be disclosed only to
17 individuals who both possess the requisite clearance and additionally have a need to
18 know the information at issue. See Executive Order 13526, §§4.1(a) and 6.1(dd);
19 United States v. Sedaghaty, 728 F.3d 885, 908-09 (9th Cir. 2013); United States v.
20 Mejia, 448 F.3d 436, 458 (D.C. Cir 2006); Baldrawi v. Dept. of Homeland Security,
21 596 F. Supp. 2d 389, 400 (D. Conn. 2009) (counsel without need to know properly
22 denied access to classified information despite holding a security clearance): United
23 States v. Libby, 429 F. Supp. 2d 18, (D. D.C.), amended, 429 F. Supp. 2d 46 (D. D.C.
24 2006) (security clearance alone does not justify disclosure because access to classified
25 information is permitted only upon a showing that there is a "need to know").

26 Here, the court reviewed all materials submitted under seal and concluded that
27 such ex parte proceedings are authorized by CIPA, Fed.R.Crim.P. 16(1), and the
28

1 common law.⁸ Again, the court is mindful of the argument that denial of access to the
2 FISA and CIPA materials is inconsistent with the adversary process. However, to
3 mitigate the denial of access to the classified materials and to assist the court in its
4 review of CIPA-related materials for purposes of Brady, the First and Fourth
5 Amendments, Fed.R.Crim.P. 16, and the Jencks Act, the court requested, and carefully
6 considered, Defendants' jointly submitted sealed memorandum identifying seven broad
7 defense theories as well as specific evidence sought to be discovered in the
8 Government's CIPA §4 submissions. (Ct. Dkt 133-35). Ultimately, for the reasons
9 set forth in the previously filed sealed CIPA orders, the court concluded that certain
10 materials were not helpful to the defense (either because the materials were not relevant
11 or cumulative to other materials already produced to Defendants) and, as to those
12 relevant and helpful statements, the court ordered the Government to provide
13 substituted statements that conveyed the material substance of those statements.

14 Accordingly, the court declines to order the Government to produce FISA- and
15 CIPA- related materials to Defendants.

16 Discovery-Related Issues

17 Defendants argue that the Government seized items (intercepted conversations
18 and telephony metadata) from Defendant Moalin but did not produce them in discovery
19 as required by Fed.R.Crim.P 16. The Government responds that it fully complied with
20 its discovery obligations under Rule 16 and that the interceptions and metadata were
21 obtained via third parties and therefore no violation occurred. The court notes that
22 Defendants fail to identify any evidence not produced by the Government pursuant to
23 Rule 16, the Jencks Act, or Brady.


24
25 ⁸ "The Government has a compelling interest in protecting both the secrecy of
26 information important to our national security and the appearance of confidentiality so
27 essential to the effective operation of our foreign intelligence service." CIA v. Sims,
28 471 U.S. 159, 175 (1985). To that end, CIPA Section 4 expressly authorizes the United
States to submit an ex parte motion seeking in camera review of classified information
that may be discoverable in a federal criminal case. 18 U.S.C. App. III § 4. The Ninth
Circuit has endorsed the ex parte proceedings as an appropriate means of reviewing
classified information under CIPA § 4. United States v. Klimavicius-Viloria, 144 F.3d
1249 (9th Cir. 1998).

1 Defendants also argue that the Government failed to comply with its obligations
2 under Brady to produce exculpatory information. Among other things, Defendants
3 seek to discover the reasons underlying the conclusion of the 2003 investigation
4 involving Defendant Moalin; evidence that Defendant Moalin's contacts with al
5 Shabaab were indirect, not direct; exculpatory evidence concerning the earlier Anaheim
6 investigation of Defendant Nasir; and exculpatory evidence related to the so-called FIG
7 assessment. The Government responds that it has complied with its obligations under
8 Brady and produced to Defendants all such materials. The court notes that the court
9 has ordered the Government on several occasions - most recently in its January 30,
10 2013 order - to comply with its obligations under Brady. (Ct. Dkt. 273). Based upon
11 the court's careful review of all materials provided by the Government under FISA and
12 CIPA, as well as the myriad of intercepted communications provided to the defense,
13 the court has no reason to suspect or speculate that the Government may have faltered
14 in its Brady obligations. The current defense requests for further discovery ignore the
15 timing and nature of the involvement of these Defendants which led to their
16 convictions, which, in turn, were supported by strong and compelling evidence. As
17 Defendants fail to identify any discovery or Brady violation by the Government, the
18 court denies the motion for new trial based upon alleged discovery violations.

19 In sum, the court denies the motion for a new trial in its entirety.

20 **IT IS SO ORDERED.**

21 DATED: November 18, 2013

22 
23 Hon. Jeffrey T. Miller
United States District Judge

24 cc: All parties
25
26
27
28